Exhibit 6

EXECUTIVE SESSION

PERMANENT SELECT COMMITTEE ON INTELLIGENCE,

U.S. HOUSE OF REPRESENTATIVES,

WASHINGTON, D.C.

INTERVIEW OF: SHAWN HENRY

Tuesday, December 5, 2017

Washington, D.C.

The interview in the above matter was held in Room HVC-304, the Capitol, commencing at 2:00 p.m.

Present: Representatives Conaway, Stewart, Schiff, Speier, Quigley, Swalwell, and Castro.

Appearances:

For the PERMANENT SELECT COMMITTEE ON INTELLIGENCE:

[redacted]

For CROWDSTRIKE:

DAVID C. LASHWAY, PARTNER

BAKER & MCKENZIE LLP

815 Connecticut Avenue, N.W.

Washington, D.C. 20006

For the DEMOCRATIC NATIONAL COMMITTEE:

GRAHAM M. WILSON, PARTNER

PERKINS COIE POLITICAL LAW GROUP

700 13th Street, N.W.

Suite 600

Washington, D.C. 20005

[redacted] Good afternoon. This is a transcribed interview of Shawn Henry. Thank you for speaking with us today. For the record, I am [redacted] of the House Permanent Select Committee on Intelligence. Also present today from HPSCI are Congressman Stewart and Congressman Conaway and Ranking Member Schiff, Congressman Swalwell and Congressman Castro.

Before we begin, I want to state a few things for the record. The questioning will be conducted by members and staff. During the course of this interview, members and staff may ask questions during their allotted time period. Some questions may seem basic, but this is because we need to clearly establish facts and understand the situation. Please do not assume we know any facts you have previously disclosed as part of any other investigation or review.

This interview will be conducted at the unclassified level.

During the course of this interview, we will take any breaks you desire.

We ask that you give complete and fulsome replies to questions, based on your best recollections. If a question is unclear or you are uncertain in your response, please let us know. And if you do not know the answer to a question or cannot remember, simply say so.

You are entitled to have a lawyer present for this interview, though you are not required to. I understand that you are represented by counsel, and for the record, we'd ask them to state their details.

MR. LASHWAY: Thank you. I'm David Lashway with Baker McKenzie, counsel to CrowdStrike.

MR. WILSON: Good afternoon. My name is Graham Wilson. I'm at Perkins Coie, counsel to the DNC.

[redacted] The interview will be transcribed. There is a reporter making a record of these proceedings so we can easily consult a written compilation of your answers.

Because the reporter cannot record gestures, we ask that you answer verbally. If you forget to do this, you might be reminded to do so. You may also be asked to spell certain terms or unusual phrases. Consistent with the committee's rules of procedure, you and your counsel, upon request, will have a reasonable opportunity to inspect the transcript of this interview in order to determine whether your answers were correctly transcribed.

The transcript will remain in the committee's custody. The committee also reserves the right to request your return for additional questions should the need arise.

The process for the interview is as follows: The majority will be given 45 minutes to ask questions. Then the minority will be given 45 minutes to ask questions. Immediately thereafter, we will take a 5-minute break, after which, the majority will be given 15 minutes to ask questions and the minority will be given 15 minutes to ask questions. These time limits will be strictly adhered to by all sides with no extensions being granted. Time will be kept for each portion of the interview, with warnings given at the 5-minute and 1-minute mark respectively.

To ensure confidentiality, we ask that you do not discuss the interview with anyone other than your attorney.

You are reminded that it is unlawful to deliberately provide false information to Members of Congress or staff.

Lastly, the record will reflect that you are voluntarily participating in this interview, which will be under oath. I will now go ahead and swear you in.

[Witness sworn.]

[redacted] Thank you.

[redacted]

MR. CONAWAY: Hang on. The fact that you didn't raise your right hand, is that significant at all?

MR. HENRY: No, sir.

MR. CONAWAY: That doesn't take the --

MR. HENRY: I swear to tell the truth. My hand is up.

MR. CONAWAY: Adam, any comments?

MR. SCHIFF: No. Welcome. Appreciate you coming in.

MR. CONAWAY: Shawn, do you have an opening statement?

MR. HENRY: No, sir, other than I've been in this room many times in my prior life in the FBI. I've spoken before this committee, coincidentally, about cybersecurity, many times over the last probably 8 or 10 years. And I appreciate what the committee is doing. I want to sit here and talk to you about the facts, as I know them, and to provide any information that would be of value to you.

MR. CONAWAY: Well, thank you.

We'll start with Chris. Thank you, sir.

MR. STEWART OF UTAH: Thank you, Mr. Henry, for joining us, for your counsel as well. And the good news for you, sir, is that I'll be leading some of the questioning today, and I'm not an attorney. And I think --

MR. HENRY: Thankfully. Sorry.

MR. STEWART OF UTAH: I think that you'll see maybe different circumstances or the questioning will be much less formal. And, again, I'm not an attorney nor a prosecutor as some have. We just want to try and get some

information and background on you or from you, and we look forward to learning more on what turns out to be one of the pivotal and one of the -- you know, one of the most important elements as we look at what's happened over the last, you know, 14 or 15 months.

So maybe you could begin by describing your relationship with the DNC, if you would, and specifically understanding that you were hired by the DNC subsequent to the hacking of their servers during the 2016 election. Could you give us some background on, again, your relationship with them, your professional relationship, the dates, and how long that's existed?

MR. HENRY: Yes, sir. I worked with Michael Sussmann, who is counsel at Perkins Coie, when I was in the FBI, in the FBI Cyber Division, probably back in the early 2000s. Michael was an attorney at the Computer Crime and Intellectual Property Section at the Department of Justice, where I knew him. We had just a professional relationship. I don't have any recollection of ever socializing. So -- but I did see him for lunch a couple of months before he called me for this. It was just to catch up; how are you?

MR. STEWART OF UTAH: And when was this?

MR. HENRY: I would say in early 2016. It may have been the wintertime, January or February, prior to the call. Just telling him what I was doing in the private sector. I would occasionally bump into him at an event at the Department of Justice or some like a holiday party, that sort of thing. But we didn't have a social relationship.

He contacted me in -- as it relates to this matter, April 30th of 2016. And he said that he had a client and they had seen some unusual activity in their -- in their network environment. And he asked if we were able to help them, if I was

able to help them with my team. He was aware that we do cybersecurity, we have developed technology that helps to identify attacks in environments, and that we also do incident response services where, when we identify or when an attack is identified we come in and help the organization identify the methodology by which to remediate the network.

MR. STEWART OF UTAH: And did he describe it as unusual activity?

MR. HENRY: That's my characterization. He was concerned that there was something going on. He didn't -- I think on April 30th, I don't think he told me that it was the DNC, but it was a client. I contacted -- if I recall correctly, he sent me an email. I was on a plane. I told him I'd call him when I landed.

And then, when I landed, I did contact him by phone. He may have said it was the DNC then. But he wanted to talk to me and my team about -- about coming in and doing an evaluation or an assessment of their network.

MR. STEWART OF UTAH: So he may or may not have described the client as the DNC, but I want to clarify. Did he describe it as unusual activity, or did he say, I have a client who's been hacked, or did he give you background on what his concerns were?

MR. HENRY: I don't recall what his words were, but the implication to me was he had a client who had been hacked. And I don't remember exactly what he said, but that was the implication.

MR. STEWART OF UTAH: Okay. Because they -- would they have known that at that point, that they'd been hacked? And if they would have, do you know how they would have known that?

MR. HENRY: So it depends. Would they have known it? It depends on what they may have seen, if they saw some type of unusual traffic at the network

layer.

I subsequently became aware that they had been contacted previously by the FBI. So I think, in looking at the communications they had with the FBI and then whatever traffic that they saw or unusual activity, it led them to believe that they needed to contact somebody to do a full examination of the environment.

MR. STEWART OF UTAH: Okay. And as I recall, the FBI initiated contact with them. Is that your understanding?

MR. HENRY: That is my understanding, yes, sir.

MR. STEWART OF UTAH: And that was conveyed to you as well?

MR. HENRY: By Michael Sussmann, yes, sir.

MR. STEWART OF UTAH: Yeah, yeah. And do you know anything about the substance of that contact, what information was shared by the FBI with the DNC?

MR. HENRY: I do know after the fact, not before. Sussmann talked to me, and it would have been over the course of a couple of days from April 30th, when he first contacted me and said, I have somebody that I want you -- a client that has a problem or an issue. I contacted him that night and then shared -- had a couple members or at least one member from my team get on the phone with him the next day on May 1st to talk about it. And then he had shared with me some of the substance of the communications between he and -- or the DNC and the FBI.

MR. STEWART OF UTAH: Okay. Maybe -- I have some questions, but I'll follow up. Maybe if you'd just continue the narrative. So you have a phone call from an associate, and he says, you know, we have some problems we're worried about. And then did he contract with you at that point or --

MR. HENRY: Yes. Over the course of the next day or two, we talked about what a contract would look like and us coming in to initiate an evaluation of their network.

MR. STEWART OF UTAH: Okay. And can you describe for us the terms of that contract?

MR. HENRY: In terms of?

MR. STEWART OF UTAH: Like duration, for example. I mean, I don't think we're particularly interested in the financial value of the contract. Maybe others are. But, I mean, mostly the duration, or was it just "Come look at this one thing," or was it --

MR. HENRY: I think that -- well, typically -- and I don't recall specifically, but typically it's, you know, a bucket of hours. You know, we'll come in for a hundred hours at X number of dollars, and we'll do an evaluation, and then we'll make a determination after that initial triage what other steps might be necessary.

MR. STEWART OF UTAH: Okay. And was this work that you would do yourself or you would have your employees?

MR. HENRY: My employees. I would not.

MR. STEWART OF UTAH: Was it unusual to you in your line of work for a client to say they'd been contacted by the FBI or by any law enforcement agency and be told, we think you've been hacked? Is that --

MR. HENRY: That's not unusual.

MR. STEWART OF UTAH: It happens frequently?

MR. HENRY: Periodically, I would say. I wouldn't say frequently, but periodically.

MR. STEWART OF UTAH: And I guess at that point, the FBI doesn't offer

to remedy that. They're just advising them, right?

MR. HENRY: The FBI will typically provide intelligence information or direction or guidance, but they will not do what we would call a remediation.

MR. STEWART OF UTAH: And what is a remediation?

MR. HENRY: A remediation is coming in to do a technical analysis of the environment and then, if identifying an adversary on the environment, taking steps to essentially build a new environment and moving the adversary off of the old environment.

MR. STEWART OF UTAH: So help me understand. I don't want to come back to that, because I don't understand that well, but I think I got enough to go on for now. Help me understand if they suspect a hack has occurred, which is criminal activity, true?

MR. HENRY: Yes.

MR. STEWART OF UTAH: So there's a crime that's been committed. Why would not the FBI have at least some role in the investigation subsequent to that hack?

MR. HENRY: So why would the FBI not have a role?

MR. STEWART OF UTAH: Yeah. I mean, they said: Hey, they contact them. You've been hacked, which is a crime. I don't understand why the FBI wouldn't lead or at least have some role in investigating the evidence associated with that crime.

MR. HENRY: So -- excuse me one minute, because I have something I --

So, just to preface my statement, because I think it's important, one piece to understand. Typically, the FBI looks at computer intrusions, based on, from a national security perspective as well as a criminal perspective. And actions they

may take in an environment are often directed by that, who the actors may be -- generally, the FBI.

As it relates to this case, we shared intelligence with the FBI. We had contact with them over a hundred times in the course of many months from June of 2016 up through current time, in the last couple weeks, I imagine.

MR. SWALWELL: A point of order. My understanding is this interview was unclassified. Is that right? Can we just clarify if the witness had classified -- my sense is that there's some sensitivities around classified information, and this setting is part of the issue. That's just what I'm --

MR. STEWART OF UTAH: I'm not sure I understand his --

[redacted] There hasn't been anything classified said so far.

MR. SWALWELL: I don't understand. It looks like he may have classified information to share, and that's the issue.

MR. HENRY: I'm not sharing any classified information.

MR. SWALWELL: I guess through questions, I think it may be touching on that.

MR. STEWART OF UTAH: Okay. Answer as best you can I guess is all I can say, but let's be careful in your -- does your -- for further background, does your firm work in classified, and do you have security clearances?

MR. HENRY: There are people on my team who have security clearances, including me.

MR. STEWART OF UTAH: Okay. Active security clearances?

MR. HENRY: Yes, sir.

MR. STEWART OF UTAH: That allows you access to SC or above?

MR. HENRY: I do have an active security clearance. And just to clarify,

do you know what my background is?

MR. STEWART OF UTAH: I do, yes.

MR. HENRY: So I mean, I ran that program. So it's --

MR. STEWART OF UTAH: Right.

MR. HENRY: So I do have a clearance, but there's nothing that I've said that's classified.

MR. STEWART OF UTAH: Yes. And I appreciate, Eric, your -- you know, we want to keep this in the proper setting.

MR. HENRY: Understood.

MR. STEWART OF UTAH: And if there's questions -- or if there's information especially that you believe is relevant and we need to, you know, arrange an interview in a different setting, we'd certainly be willing to do that.

MR. HENRY: Yes, sir.

MR. STEWART OF UTAH: Okay. Let me go back, if I could, to where I'm trying to understand. And I'm really not -- this isn't a "got you" kind of thing. I have no "got you" here. I'm just trying to figure this out.

So, if my questions seem uninformed, I'm admitting to you that they are, because I don't have a background in this. It just is interesting to me, and it seems, I don't want to say inconsistent, but curious to me that there would be evidence of a crime and that there wouldn't -- and especially with a client. Now, you may not have been aware of the client initially, but you quickly became aware of the client.

MR. HENRY: Very quickly.

MR. STEWART OF UTAH: Yeah. I mean, this isn't Joe's Pizza. This is something else with much more intense, I don't want to say national security, but

political and other interests. I mean, this client is, after all, a national figure in the middle of a national campaign.

Did it strike you as curious or -- that the FBI didn't take the lead in this investigation? And who makes that decision? Does the FBI -- let me ask you this way: In your experience, whether in your official capacity in the government or now as a private contractor/business owner, do you have examples of where something similar like this happened, but the FBI or any other law enforcement organization came in and said, "we're going to take the lead on this, this is a criminal matter, we're going to do the investigation"?

MR. HENRY: In these types of cases, my experience typically has been notification made to the victim about what has occurred in their environment, not that the FBI would typically come in. And they certainly wouldn't conduct a remediation. And they --

MR. STEWART OF UTAH: And remediation is protecting the --

MR. HENRY: Remediation is essentially cleaning it up. Something bad has happened. There's been an actor. There's malware, malicious software in an environment. Somebody has access to what's occurring in the environment. So the remediation is cleaning out the bad stuff and putting in place infrastructure that is safe and secure.

MR. STEWART OF UTAH: So, in this case and generally, it's to protect the client. It's to protect their security from that point forward as best they can.

MR. HENRY: Yes, sir.

MR. STEWART OF UTAH: Okay. So you were saying that generally, they -- the FBI doesn't do remediation, but --

MR. HENRY: They make notification.

MR. STEWART OF UTAH: Okay.

MR. HENRY: They often collect intelligence that's of value to the broader Intelligence Community.

MR. STEWART OF UTAH: Okay. And were they able to do that in this case?

MR. HENRY: I don't know what they had access to in the environment. I can tell you that the intelligence that we shared with them, including forensic information, indicators of compromise, which are pieces of malware, et cetera, we provided all of that to the FBI. Starting in June of 2016, we provided them the data that would have been of value to them.

MR. STEWART OF UTAH: Okay. Did they indicate to you at any time who they suspected or who they feared, any inference at all about who might have been responsible for this hack, or these hacks?

MR. HENRY: I don't recall when we came in. There had been some I mentioned notification to the DNC in the months prior to the phone call that I received from Sussmann. When Michael Sussmann provided me with information that the FBI had contacted the DNC, he said that they had told him -- they used a term that I know is related to the Russian Government.

MR. STEWART OF UTAH: And that was -- I'm sorry, that was when, at what point in this relationship or this work?

MR. HENRY: I found that out from Sussmann the first day or two after he made notification, so April 30th or May 1st of 2016, but that that notification had been made to the DNC months prior.

MR. STEWART OF UTAH: Okay. So the DNC is notified by the FBI that they've been hacked and that they believe the hack occurred by a foreign

government, in this case Russia.

MR. HENRY: So let me -- yes, but let me clarify, if I could. When we say "the DNC," my understanding is there was a contractor who was administering the network for the DNC, and he was the one that had been contacted by the FBI for months leading up to the phone call that I got from Michael Sussmann.

MR. STEWART OF UTAH: Okay.

MR. HENRY: So when I -- I want to be clear. When I say the DNC, he wasn't a DNC employee. He was a contractor that was administering the network for the DNC.

MR. STEWART OF UTAH: All right. So I want to make sure I understand this. So DNC exists. They have a network. They have a contractor providing security for that network. That contractor is notified by the FBI that there's been a breach and that they believe the breach occurred, or a hack, by the Russian Government.

MR. HENRY: So the -- so the term that the contractor -- the contractor said that the FBI told him the Dukes, D-u-k-e-s, was identified. I don't know if the contractor knew that the Dukes were associated with the Russian Government.

MR. STEWART OF UTAH: Is that a common term, the Dukes?

MR. HENRY: It's a -- oftentimes, adversaries are given a code name or some type of a reference, and that people in the industry become familiar with the nomenclature. And the Dukes is a common term associated with an actor that many people who work this type of -- do this type of work in the private sector refer to that Russian actor as.

MR. STEWART OF UTAH: Okay. So it's not just the FBI or just your office. I mean, someone who worked professionally --

MR. HENRY: Yes, sir.

MR. STEWART OF UTAH: -- and is competent in this industry would know what the Dukes were?

MR. HENRY: Yes, sir.

MR. STEWART OF UTAH: And you would have expected this contractor to know what the Dukes were --

MR. HENRY: Well --

MR. STEWART OF UTAH: -- assuming that they were --

MR. HENRY: So, when I say "people who work in the industry," I'm referring to people like my company and others that respond to these types of incidents. I don't know what the contractor's security proficiency was or what his access to other types of information was.

MR. STEWART OF UTAH: So your understanding is that, when the FBI contacted this contractor, they may or may not have said Russia, but you believe they did say the Dukes. Is that true?

MR. HENRY: That is true.

MR. STEWART OF UTAH: But they might have said Russia, you just don't know?

MR. HENRY: I don't know that.

MR. STEWART OF UTAH: Okay. Is there any reason you believe it was just the Dukes and not Russia or -- I mean, did they indicate to you after in subsequent conversations what they were told?

MR. HENRY: He said the Dukes.

MR. STEWART OF UTAH: But when he said it with you, he indicated he knew who the Dukes were at that point?

MR. HENRY: So that's not -- I wouldn't say that. I saw what I saw -- let me be clear here, because as you and I are speaking I'm saying "he said." There was a document that I read that was a summary from the contractor of his communications with the FBI. I read the document. I never personally spoke with the contractor, but I read the document that I was told the contractor wrote.

MR. STEWART OF UTAH: Got you.

MR. HENRY: Which was essentially a chronology.

MR. STEWART OF UTAH: Got you. And that makes it harder to infer meaning into words other than what you might have been able to pursue more in a conversation.

MR. HENRY: Yes, sir. But the word "Dukes" was in the document.

MR. STEWART OF UTAH: I understand. Okay. Let me go back, if I could, just a little bit. I want to understand better your experience, again, both officially as a government agent and now in the private sector. If an entity like the DNC or any, you know, organization that has the obvious impact or import of the DNC had been informed that they had been hacked and by -- hopefully they understood -- by a foreign government, what would that organization typically do? I mean, wouldn't law enforcement at some point be involved with that investigation? And, again, I've asked this question before. I just want to -- I don't think we got a chance to fully answer it.

MR. HENRY: So I'm sorry, if you could repeat the question.

MR. STEWART OF UTAH: Well, I'm just kind of framing it up. Again, we have an organization, a very important national organization has been informed by a law enforcement agency, in this case the FBI, that they have been hacked and, in fact, hacked by a foreign government.

It would seem to me that the FBI or some legal and investigative -- you know, official investigative body would be involved with that. Am I misreading that? What makes that assumption on my part fallacious?

MR. HENRY: I don't think it is. When you ask, though, about the DNC being notified, again, my understanding is the only person that was notified was the contractor. At what point officials in the DNC became notified, I'm not aware of that.

MR. STEWART OF UTAH: Okay. That actually -- let me pursue that line, if I could. I'm sorry. Did you want to --

MR. HENRY: No. I mean, just to go back to a comment I made earlier about the FBI and the investigation, that we did provide the FBI with information. They were conducting an investigation. Whether they were feeding back information to the DNC or not, I don't know, but they were conducting an investigation, to my understanding. And when we sat with them in June, we provided them with a lot of the indicators, the malware, and other pieces of code that we took off of the computer network.

MR. STEWART OF UTAH: Okay. Could they conduct their own investigation in a thorough fashion without access to the actual hardware?

MR. HENRY: Maybe. It depends on what else they had access to. They may have if they had access to other pieces of information.

MR. STEWART OF UTAH: What else could -- I mean, what other pieces of information would allow them to do a complete investigation without access to the hardware that was hacked?

MR. HENRY: So, right, we're in an unclassified environment, and I would be speculating. But having been in that space, I could tell you in a different

environment.

MR. STEWART OF UTAH: Okay. Maybe we'll follow up with you on that then. Let me ask you just to surmise. Are you comfortable that someone could complete a thorough investigation, using other tools, without direct access to the hardware or the equipment?

MR. HENRY: Could they come to a conclusion? You're asking a nuanced question. And I'm not being cagey. I want to be clear, because this is an important point.

MR. STEWART OF UTAH: Well, let me rephrase that, and it will maybe make it simpler. Would it be better if they had access?

MR. HENRY: As an investigator, and I've been an investigator for almost 30 years, the more information you have access to, the better in any investigation. But it doesn't mean that a lack of a piece of information precludes you from coming to a conclusion.

MR. STEWART OF UTAH: And I could see that. So let me surmise this and tell me if this is wrong: You could have a better investigation if you had access to all of the equipment or hardware or whatever that was available. You would be able to do a better investigation.

So the question is, would there be reasons for not making that available that override the benefit of having a more conclusive investigation? Is that a fair summary? If someone wasn't going to make that available, they would have to have reasons for not doing that because they would likely have a less thorough investigation by not making it available?

MR. HENRY: You're asking me to speculate. I don't know the answer.

MR. STEWART OF UTAH: By the way, you need to pay him well,

because he's obviously serving you well today as you guys have your conversations back and forth together.

MR. HENRY: I want to be very clear on what I'm telling you. It's important to me.

MR. STEWART OF UTAH: Okay. I appreciate that. And we do; we want clarity. And by the way, when we're talking, you know, on the edge of, you know, very sensitive subjects, we appreciate that you're being careful.

MR. HENRY: That's all.

MR. STEWART OF UTAH: And believe me, we understand that. I have a lot of conversations when I think, "Oh my gosh, did I say something I shouldn't have." I think we all have.

Could we talk a little bit about the memo that was provided you, and you said it laid out -- I believe you said it laid out the information that you -- and that's where you first heard the reference to Dukes.

MR. HENRY: Yes, sir.

MR. STEWART OF UTAH: Could you give us kind of the content of that memo and surmise what it told you?

MR. SCHIFF: May I ask a question? Any reason we don't want to do this in classified session when he can answer all these questions without having to worry about what's classified and not classified? Any reason we don't want to do that in a classified session?

MR. STEWART OF UTAH: Counsel is not cleared.

MR. SCHIFF: Counsel is not cleared. Thank you, Mr. Chairman. Sorry to interrupt.

MR. STEWART OF UTAH: How much time?

[redacted] You have 25 minutes.

MR. STEWART OF UTAH: So 20 down?

[redacted] Excuse me, 20 minutes.

[redacted] Ten till.

MR. SCHIFF: Mr. Stewart, you missed your vocation. You're doing an excellent job on your questions.

MR. STEWART OF UTAH: Oh, thank you. I dream of being an attorney one day, right? I'm not smart enough.

MR. CONAWAY: Prosecutor, actually.

MR. STEWART OF UTAH: I'm not smart enough for this.

MR. CONAWAY: Go all in.

MR. STEWART OF UTAH: I don't know if I asked -- oh, I asked you for the chronology. You just said the synopsis of what the memo that was provided you. If you could tell us, you know, what information it gave you.

MR. LASHWAY: Just for the record, some of the comments we were just discussing, as Mr. Henry indicated, certain of the work that was performed was performed at the behest of counsel, Perkins Coie, Mr. Sussmann's law firm. Therefore, certain of that information, the DNC, as the client of Perkins Coie, has asserted privilege and some confidences over certain of that information, sir.

And so we would turn to Perkins Coie, as counsel to the DNC, to ensure that Mr. Henry can actually answer some of these questions relating -- some of that information that would otherwise be considered protected by the DNC, as the client.

MR. STEWART OF UTAH: Okay. Counselors.

MR. LASHWAY: I apologize.

MR. WILSON: Yes, thank you. And on behalf of the DNC, the DNC takes the work of this committee and this investigation incredibly seriously. It was the victim of, you know, a horrible intrusion and wants to cooperate in every way that we can in order to provide this committee all the information it needs to get back.

So, as Mr. Lashway referenced, CrowdStrike was working for Perkins Coie and was performing work in order to help Perkins Coie advise the DNC on this matter.

MR. STEWART OF UTAH: If I can just clarify one thing you said. CrowdStrike was working for Perkins Coie. Is that the contract was actually with the law firm then?

MR. WILSON: Correct. We had a contract between Perkins Coie and CrowdStrike, with a scope of work for the DNC-specific work.

MR. STEWART OF UTAH: So does that mean that you never had a contract, Mr. Henry, with the DNC directly then?

MR. HENRY: I mentioned it was with Michael Sussmann from Perkins Coie.

MR. STEWART OF UTAH: Good. Thank you.

MR. WILSON: So the one thing I would want to say is I think we are not waiving any of the attorney-client privilege over the work product here today. That being said, we are trying to -- you don't hear me piping up, "don't say this," "don't say that," because we want Shawn to be able to give you the information that was relevant to this investigation so you have it.

MR. STEWART OF UTAH: Yes.

MR. WILSON: And we're happy to have him do that. And without -- again, I'm not waiving any privilege, we're happy to have him continue to

go. With the request for a specific document and the contents, you know, like that that was a DNC document, if you want to put that question to the DNC, we'd be -- I'd be happy to discuss that with him and we can come back to it.

MR. STEWART OF UTAH: Well, that seems perfectly fair. And we'll talk with counsel and get back to you on whether we'd like to request a document. Could I ask this: I mean, can you share any information with us just in regards to the work and how you started that work? Did the memo help you get started or did it share information with you that, you know, would not violate client privilege that, you know, would be helpful to this committee to understand?

MR. WILSON: I'm fine with you answering that.

MR. HENRY: It was a chronology of FBI communication with the contractor. He'd been called over the course of several months. He'd been contacted. And it just summarized different phone calls and different meetings he had with the FBI.

MR. STEWART OF UTAH: So it was more detailed, but essentially what you've told us up to this point, basically?

MR. HENRY: Yes, sir.

MR. STEWART OF UTAH: Was there ever indication or evidence that the contractor had communicated what he knew -- because that's one of the central questions -- what he knew -- to the leadership of the DNC?

MR. HENRY: I don't -- I don't recall that being in the document, and I don't have any knowledge or any recollection of that.

MR. STEWART OF UTAH: Okay. So, as far as you know today, he may or may not have communicated immediately to the DNC, or he may have never communicated to the DNC? You don't know?

MR. HENRY: I don't know.

MR. STEWART OF UTAH: Could you -- would you maybe just continue with your narrative then. So your initial contact told this information and you begin your work within a few days, as I understand it.

MR. HENRY: Yes.

MR. STEWART OF UTAH: And would you just conclude with what you discovered and how you discovered it and what you did with that information?

MR. HENRY: So we did -- we did some forensic analysis in the environment. We deployed technology into the environment, into the network, software called Falcon that essentially looks at the processes that are running on different computers in the environment.

We also looked historically at the environment, using a different piece of software to look backwards at what was happening in the environment. And we saw activity that we believed was consistent with activity we'd seen previously and had associated with the Russian Government.

MR. STEWART OF UTAH: And can you identify that as being -- with a fair degree of confidence that it's associated with the Russian Government?

MR. HENRY: We said that we had a high degree of confidence it was the Russian Government. And our analysts that looked at it that had looked at these types of attacks before, many different types of attacks similar to this in different environments, certain tools that were used, certain methods by which they were moving in the environment, and looking at the types of data that was being targeted, that it was consistent with a nation-state adversary and associated with Russian intelligence.

MR. STEWART OF UTAH: Okay. Are there other nation-states that

could have -- based on this evidence, that could have been the perpetrator?

MR. HENRY: There are other nation-states that collect this type of intelligence for sure, but the -- what we would call the tactics and techniques were consistent with what we'd seen associated with the Russian State.

MR. STEWART OF UTAH: And so, because I'm not familiar with this, I'm trying to give it a little more context. You said high confidence or high degree of confidence. We use that phrase in the IC, as you know, and it means, you know, something, but it's not, you know, absolute in its meaning.

And so an analogy might be a fingerprint. You know, if you have a fingerprint and I know that that fingerprint's a match -- and I understand kind of because of my life and just being alive and knowing -- that's fairly accurate, a high degree of confidence.

Is that the same level of confidence as a fingerprint, or is it something less than that, in your ability to define it as the Russian Government?

MR. HENRY: There wasn't a videotape --

MR. STEWART OF UTAH: Yeah.

MR. HENRY: -- of the Russians with their fingers on a keyboard, but the activities were consistent with what we'd seen previously, targeting other -- the State Department, for example, the Joint Chiefs, other governments, Western governments. And it was consistent with what we'd seen previously and associated with the Russian Government.

MR. STEWART OF UTAH: Okay. And in those other instances you mentioned, was there any subsequent evidence that verified it really was the Russian Government that maybe wasn't found in this case? In other words, you can make your initial analysis: we think this is the Russian Government. Then, as

time plays out, you have other evidence that proves, yeah, it was the Russian Government. I'm sure that's been the case in some cases, right?

MR. HENRY: I think that when you're looking at attribution, it's -- you look at an aggregate across many different attacks over a long period of time, years in many cases, and the intelligence that you collect leads you to a certain conclusion. I think that's the case here.

MR. STEWART OF UTAH: Okay. I have just a few more questions. Then I'll see if the chairman wants to follow up on anything.

Kind of encapsulating, and I think I understand the narrative you've laid out. Well, I tell you what: Mr. Henry, conclude, would you please? So you started, you did your analysis. You drew your conclusions, and that took about how long?

MR. HENRY: So the analysis started the first day or two in May, and then that was about 4 to 6 weeks. I think, on June 10th, we started what we call the remediation event. So we collected enough intelligence. We identified where the adversaries were in the environment. We came up with a remediation plan to say we see them in multiple locations. This -- these are the actions that we need to execute in order to put a new infrastructure in place and to ensure that the adversaries don't have access to the new infrastructure.

So that would have been June 10th when we started. And we did the remediation event over a couple of days.

MR. STEWART OF UTAH: And while you're investigating from May to June, is the DNC, is the client still vulnerable at that time?

MR. HENRY: Yes.

MR. STEWART OF UTAH: And is the adversary aware, are they able to see your activities?

MR. HENRY: The idea is that they don't. We don't know if they did. We don't have any indication that they did, because we want to be surreptitious for that very reason.

MR. STEWART OF UTAH: Okay.

MR. HENRY: So that they don't take actions.

MR. STEWART OF UTAH: Yeah.

MR. HENRY: I don't have any reason to believe that I can recall that we thought they knew.

MR. STEWART OF UTAH: Okay. So, at the end of the 6 weeks, you've concluded your work or close to it?

MR. HENRY: To be clear, our goal, my goal was to protect the client. We were hired to protect the client. We identified an adversary there. The goal was to make sure that the adversary was removed and the client had a clean environment with which to work.

MR. STEWART OF UTAH: And at the end of that period, you feel you'd been able to accomplish that?

MR. HENRY: At the end of June, June 12th, when we did the remediation event, yes. But we also know that it is common for an adversary to try and reacquire a network when they're moved off. That's common knowledge in this business. So we had technology deployed that would help us identify if they were back in.

MR. STEWART OF UTAH: And, to your knowledge, they were not able to after June 12th?

MR. HENRY: There was another activity in the environment. We didn't do direct attribution back in that case. They were different tools that were not

similar or consistent with what we'd seen the first time.

MR. STEWART OF UTAH: And when was that?

MR. HENRY: In September of 2016.

MR. STEWART OF UTAH: And when you say you didn't do attribution back, does that mean that you didn't attempt to or you weren't able to?

MR. HENRY: We weren't able to. We didn't -- there were different toolsets in the second, the second attack.

MR. STEWART OF UTAH: But apparently, it was --

MR. HENRY: We did -- we -- to be clear, we -- our technology -- the attack, the second breach was in an environment that had not -- did not have our technology deployed into it. When the adversary, whomever that was, when they moved to one of the computers that had our technology, we alerted and recognized that there was another attack in the environment.

MR. STEWART OF UTAH: In this case, it was unsuccessful?

MR. HENRY: No, it was not unsuccessful.

MR. STEWART OF UTAH: It was a successful breach again?

MR. HENRY: Into parts of the environment that did not have our technology in it.

MR. STEWART OF UTAH: Okay. And then did that lead to another remediation for you?

MR. HENRY: Yes, it did.

MR. STEWART OF UTAH: Looking at this kind of in its entirety -- now, let me ask you, is there anything more that you would add to, you know, your work in this regard?

MR. HENRY: More that I want to add? Can I stay all day? So --

MR. STEWART OF UTAH: And let me -- I'll narrow my question, if I could, because that's an unfair question, I mean, because -- in regards to your work with the DNC, does that -- did that conclude your work with the DNC?

MR. HENRY: I think -- I think so. I don't want to make an emphatic statement, because over the course of the next couple months, there were leaks of data. We were talking to people at the DNC. They were trying to identify what documents were being leaked. So there were certainly communications. I think we were monitoring their network. I mean, we still had our technology in their network.

So I wouldn't say it ended. But, from a professional services or an incident response perspective, probably, but we still had engagement with them, because leading up to the election, we had concerns that the Russians were going to come back or somebody was going to try to access that environment. So we did provide monitoring throughout that period of time.

[redacted] Mr. Stewart, 5 minutes.

MR. STEWART OF UTAH: Wow. So much fun, the time just flies.

Let me -- one question very quickly. There are some press reports or some people at least claim that this hack on the DNC did not -- was not perpetrated by the Russians. How do you respond to that?

MR. HENRY: Everything in my experience, sir, having done this for many, many years, both in the government and in the private sector, says that it was the Russian Government.

MR. STEWART OF UTAH: Is there anyone with -- that you think -- well, I'm not going to ask that question. Never mind.

Thinking of it in its entirety now, going back to, you know, the client, who

was -- I know the contractor, who was informed I think you said several months, if they had relied on the information provided by the FBI in a more timely fashion, because it seems to me they didn't if it was several months later that they contracted you or contacted you, could they have prevented a substantial portion of this, of this hack or this -- the outcome that was -- you know, that we see now if they had acted more -- in a more timely or more urgent manner?

MR. HENRY: If they had relied on the -- on what they had received from the FBI, had they responded earlier, could they have stopped the attack? Is that the question?

MR. STEWART OF UTAH: Or at least mitigated the damage.

MR. HENRY: Depending on how they responded, they may have.

MR. STEWART OF UTAH: If they had been proactive.

MR. HENRY: It's speculation for me to say that.

MR. STEWART OF UTAH: Well, I don't think it's an absurd speculation, I mean, because if you're informed of an attack and you act on that aggressively, you're obviously going to minimize the damage that, you know, occurs.

MR. HENRY: I think that's fair.

MR. STEWART OF UTAH: At any point, are you aware of the FBI ever asking for access to anything, whether it's coding or whether it's something you've collected or whether it's the DNC and their equipment or hardware, did the FBI ever, as far as you know, ask for access, and were they informed by the client they could not have that access?

MR. HENRY: I'm not aware of the FBI asking the DNC for data.

MR. STEWART OF UTAH: Okay.

MR. HENRY: But, just to restate, that we were in contact with them many

times, over a hundred times from June until even in the last few weeks. Provided them with information related to this attack.

MR. STEWART OF UTAH: Got you.

MR. HENRY: Including electronic data, et cetera.

MR. STEWART OF UTAH: Okay. But you're not aware of them ever asking and being denied any information or any access?

MR. HENRY: I do not have a recollection of that. I'm not aware.

MR. STEWART OF UTAH: And so, if they didn't request it or that was on their own accord, they made the decision not to request access, as far as you know?

MR. HENRY: I don't know.

MR. STEWART OF UTAH: Okay. All right. Chairman, do you have anything you want to follow up on?

[redacted] You've got 1 minute, sir.

MR. CONAWAY: No. We'll switch.

MR. STEWART OF UTAH: Thank you.

And, Mr. Henry, thanks for your response.

MR. CONAWAY: Turn it over to the ranking member.

MR. SCHIFF: Thank you, Mr. Chairman.

I just have a couple followup questions. Then I'm going to turn it over to Mr. Castro. Welcome, and thank you for coming to testify.

My colleague asked you whether the damage that was done to the DNC through the hack might have been mitigated had the DNC employed your services earlier. Do you know the date in which the Russians exfiltrated the data from the DNC?

MR. HENRY: I do. I have to just think about it. I do know. I mean, it's in our report that I think the committee has.

MR. SCHIFF: And, to the best of your recollection, when would that have been?

MR. HENRY: Counsel just reminded me that, as it relates to the DNC, we have indicators that data was exfiltrated. We did not have concrete evidence that data was exfiltrated from the DNC, but we have indicators that it was exfiltrated.

MR. SCHIFF: And the indicators that it was exfiltrated, when does it indicate that would have taken place?

MR. HENRY: Again, it's in the report. I believe -- I believe it was April of 2016. I'm confused on the date. I think it was April, but it's in the report.

MR. SCHIFF: It provides in the report on 2016, April 22nd, data staged for exfiltration by the Fancy Bear actor.

MR. HENRY: Yes, sir. So that, again, staged for, which, I mean, there's not -- the analogy I used with Mr. Stewart earlier was we don't have video of it happening, but there are indicators that it happened. There are times when we can see data exfiltrated, and we can say conclusively. But in this case, it appears it was set up to be exfiltrated, but we just don't have the evidence that says it actually left.

MR. SCHIFF: Did the technology vendor -- could you tell us who the technology vendor was that you were working with?

MR. HENRY: That the DNC was working with?

MR. SCHIFF: Yes.

MR. HENRY: His -- it's a company called MIS. And the actual contractor's name was Yared Tamine (ph). Y-a-r-e-d, I believe.

MR. SCHIFF: And did you get a sense from Mr. Tamene how specific the FBI was with their notification of a potential breach to their system?

MR. HENRY: He said that he had -- and this is off of that document so -- he said that he had received a phone call in September of 2015 and that he received a phone call in October of 2015, and I think there was another call again in November.

MR. SCHIFF: Did he tell you whether anyone actually came to visit, or were these just phone calls from the FBI?

MR. HENRY: My recollection is -- my recollection is the first 3 months was a phone call, and then subsequently he did meet with somebody. He had -- I believe there are a couple of meetings that were documented in the document.

MR. SCHIFF: And did he tell you whether the FBI had given him any specifics about what they were alerting him to or recommending any steps that the DNC should take?

MR. HENRY: Again, my recollection is that there -- the Dukes were there and that there were certain files he should look for, pieces of software. This -- the document chronicles activity from September of 2015 up until the day or a couple of days before Sussmann contacted me. So that would have been April 30th. So it's several months.

And he talks about different meetings and different phone calls between he and the FBI. I don't recall specifically without looking at the document which dates, was it a phone call or a meeting when he was told what, but he certainly was told that there was activity in the environment he needed to look for. And he in his, Tamene's chronicling of this, these meetings, said that he looked and he couldn't find it. On a couple of occasions, he says: I looked. I couldn't find

it. The FBI called. I looked. I couldn't find it.

MR. SCHIFF: Do you know whether the FBI had made any recommendation to him about what he should do with the information he was getting from the FBI?

MR. HENRY: In terms of notification or --

MR. SCHIFF: Well, do you know whether they recommended that they retain the services of a firm like yours, or were they saying, "We have indications you should look to see if you can find indications"?

MR. HENRY: I think it's the latter. I don't recall him documenting that he was told he should contact somebody outside of his organization.

MR. SCHIFF: In your report, when you stated the data was staged for exfiltration on April 22nd of last year, that would have been the first time that you found evidence that the data was staged for exfiltration?

MR. HENRY: I believe that is correct.

MR. SCHIFF: Did you have a chance to read the information that was filed in conjunction with the George Papadopoulos plea?

MR. HENRY: I did not.

MR. SCHIFF: In that information, it states that Mr. Papadopoulos was informed at the end of April that the Russians were in possession of stolen DNC or Clinton emails. If that information is correct, that would be only days after that data was staged for exfiltration?

MR. HENRY: Yes.

MR. SCHIFF: Once you were retained by Perkins Coie, did you become the -- essentially the point of contact for the FBI in the investigation of what the Russians were doing on the DNC server?

MR. HENRY: I talked to the FBI for the first time about this matter after the network was remediated. We were sure that the network was locked down. That would have been in June. The remediation took place June 10th to June 12th. I think June 13th, I contacted the Assistant Director of the FBI.

MR. SCHIFF: And I think you said either you or your firm had thereafter hundreds of contacts with the FBI?

MR. HENRY: I said more than a hundred. I don't know exactly the number, but it was phone calls, it was meetings, it was emails.

MR. SCHIFF: And during those hundred or more contacts, did the FBI ever tell you that they needed the DNC server for their own forensic analysis?

MR. HENRY: They asked us to provide to them the images of the computers and the results of our collection. They did ask for that, and we shared that with them.

MR. SCHIFF: And did they ever indicate to you that they thought that the images that you had given them or the information you had given them was incomplete for their own analysis and they required access to the servers?

MR. HENRY: I have no recollection of them saying that to me or anybody on my team, no.

MR. SCHIFF: And the DNC never communicated to you that the FBI was asking for the server?

MR. HENRY: No, sir.

MR. SCHIFF: Can you tell us a little bit about the images that you provided? What are those, in technical terms? How much -- how similar are those images to the actual server itself?

MR. HENRY: So I want to be clear. And I think they're referenced in the

report. When I say what we provided to them, there are some cases where we're providing the results of our analysis based on what our technology went out and collected.

So we have -- we have software that we send in to the environment. It collects artifacts, if you will, of what happened -- I mean, I'd equate it to shell casings or -- it's digital evidence -- and pulls it back. It's the remnants of code. And we will sort through all that, analyze that. We provided that information to the FBI.

I believe that there are a couple of actual digital images, which would be a copy of a hard drive that we also provided to the FBI. And there were -- we're talking about, I don't know the exact number, but in excess of 10, I think, hard drives. Again, I believe you've got the documents, so I don't want to say anything that's inaccurate. But it's not -- we're not talking about one drive.

[3:00 p.m.]

MR. SCHIFF: And those copies of the drives allow you to create a duplicate virtual environment as the DNC server?

MR. HENRY: Yes.

MR. SCHIFF: And at any time did the FBI indicate to you that that was unsatisfactory in terms of their own investigation?

MR. HENRY: I'm not aware of them saying that.

MR. SCHIFF: Mr. Castro.

MR. CASTRO: Thank you.

Thank you, Mr. Henry, for your testimony today. I'm going to ask you some basic questions about your own background and expertise, and then we'll get into this incident with the DNC and the DCCC and then more generally about these incidents.

First, you first began your career at the FBI. Is that right?

MR. HENRY: Yes.

MR. CASTRO: When did you first begin it?

MR. HENRY: January of 1989. Well, I actually started in the FBI as a file clerk in June of 1984. I resigned in July of 1985.

MR. CONAWAY: I thought he said 1994.

MR. HENRY: I work out a lot. I eat right.

I resigned in July of '84, and then I came back as an FBI agent in January of 1989.

MR. CASTRO: And when did you leave the FBI?

MR. HENRY: March of 2012.

MR. CASTRO: And what roles did you have at the FBI during that career?

MR. HENRY: I had 13 different positions. I'd be happy to go through the chronology if you need it.

MR. CASTRO: How about the ones that involve anything with cyber or what we're discussing today?

MR. HENRY: In 1999, I was selected to be the chief of the Computer Intrusion Unit in what was then the National Infrastructure Protection Center at FBI headquarters.

In 2001, I left there and became a supervisory special agent of the cyber squad in the Baltimore field office.

I was on the inspection staff after that, not specifically related to cyber.

I was the assistant agent in charge of the Philadelphia field office. I had some minimal oversight of cyber. I was working for -- the technical program was underneath me, technical squad.

I was the chief of staff for the head of the national security branch of the FBI, and so I had some interaction then with cyber issues.

I became the deputy assistant director of the Cyber Division in 2006. I became the assistant director in charge of the Cyber Division, so I led the FBI Cyber Division, in 2008.

I was the assistant director in charge of the Washington field office in 2010, and, in that capacity, I had the cyber program in my -- along with every other violation.

And then, in 2010, October 2010, I became the executive assistant director, so the Cyber Division was underneath me.

So I touched it from '99 until my retirement exclusively multiple years and

tangentially several years.

MR. CASTRO: And your final position as EAD of Criminal Cyber Response and Services Branch, how long were you in that role?

MR. HENRY: October of 2010 until my retirement in end of March of 2012.

MR. CASTRO: To the degree that you can talk about it, from your tenure at the FBI, did you have experience with sophisticated state-sponsored hackers or cyber attacks?

MR. HENRY: Yes.

MR. CASTRO: And cyber groups acting at the behest of or in coordination with a foreign government, even if not directly employed by security or intelligence service?

MR. HENRY: I'm sorry, say it again. I heard the second part, but I didn't understand the first part.

MR. CASTRO: Basically, did you have a -- did you work on cyber groups that were acting at the behest of or in coordination with a foreign government?

MR. HENRY: Yes.

MR. CASTRO: What about nonstate actors?

MR. HENRY: Yes.

MR. CASTRO: Can you tell us what differences you've seen between those two? One of the issues was how do you know it was Russia that is a nation-state or a state actor? What are the differences between when a state actor hacks versus a nonstate actor?

MR. HENRY: So, back to the gentleman's point of classification. I want to be careful, because what I did in the Bureau is classified, and I want to be careful not to say anything that might be in breach of my requirements back then.

MR. CASTRO: Do you want some time to think about it?

MR. HENRY: Well, I can say in general, I can say in general terms that my experience is nation-state actors are very sophisticated in the way they access networks, in the way that they maintain access to a network, in the way they move in the environment.

Typically, the type of information they target is very different from the information that is targeted by nonstate actors because their motivations are different. Nation-state actors are, in my experience -- nation-state actors are the most sophisticated actors in terms of their capabilities in accessing, exfiltrating, and moving in an environment.

MR. CASTRO: And based on your experience and to the extent you can tell us, do nation-states and nonstate actors hack for different reasons?

MR. HENRY: Well, yes, they do. They do. But that's a much longer answer. All actors have some motivation to get into an environment, whether it be the pilfering of data for financial gain, the pilfering of data for intelligence purposes, or, in some cases, we've seen adversaries who have access to networks and destroy the networks, which we might use Sony as an example.

MR. CASTRO: Some hackers also commercialize or profit off of their activity.

MR. HENRY: They pilfer that for financial gain, yes, sir.

MR. CASTRO: Let me ask you about your experience during your time at the FBI with anything related to Russia and hacking. So can you describe the nature and scope of any Russian cyber operations you tracked and investigated while at the FBI? Of course, in an unclassified setting.

MR. HENRY: I cannot.

MR. CASTRO: Okay. So anything they did with data exfiltration or cyber espionage?

MR. HENRY: [Nonverbal response.]

MR. CASTRO: Okay.

There has been prior public reporting of state-sponsored cyber operations against political campaigns prior to 2012. For instance, the Chinese reportedly hacked both the Obama and McCain campaigns in 2008.

Did you work or were you otherwise involved in the investigation of that apparent cyber espionage?

MR. HENRY: Yes.

MR. CASTRO: And, to your knowledge, did the Bureau work or offer help, assistance, or support to the campaigns?

MR. HENRY: Yes.

MR. CASTRO: To your knowledge, prior to the 2016 campaign, had you ever witnessed or observed a foreign state actor using cyber means against U.S. election campaigns, beyond espionage, to undertake an influence campaign, meddle in domestic political processes, or otherwise, quote/unquote, "weaponize" the fruits of hacking?

MR. HENRY: That is a complicated question and not something that I can talk about here. I can talk about what happened at the DNC.

MR. CASTRO: You mean you can't talk about it because some of the information is classified?

MR. HENRY: To the extent -- if I have information related to that, I wouldn't be able to talk about it here.

MR. CASTRO: All right.

Let me ask you about your time at CrowdStrike after you leave the FBI. When did you first join CrowdStrike?

MR. HENRY: The day after I retired from the FBI.

MR. CASTRO: And pardon my ignorance about the business, but was CrowdStrike already up and going, or were you one of the founders of it, or what was --

MR. HENRY: I was not a founder. CrowdStrike had started several months prior. And there were just a couple dozen employees -- two dozen employees at the time when I joined the company.

MR. CASTRO: How many employees are there now?

MR. HENRY: About 840.

MR. CASTRO: What was your position when you joined?

MR. HENRY: President of CrowdStrike Services. That's a wholly owned subsidiary of CrowdStrike.

MR. CASTRO: And what does that all include? What was under your purview, what kind of work?

MR. HENRY: So, when I joined, I was the president of CrowdStrike Services. My charge was leading our professional services organization, so consultants who would assist organizations in identifying adversary activity in their environment from a --

MR. CASTRO: Let me ask you, I guess, building on that, what were the services that you guys were offering your clients?

MR. HENRY: So incident response services, which is coming to a client's aid when they've been breached and helping them identify what occurred in the environment and helping them work to develop a remediation plan.

As well as proactive services, which are services done in advance to help prepare a company so that it does not become breached. So we might do a compromise assessment in an environment where we would deploy technology to help identify some deficiencies in the network so that they could prepare it. We might test the environment by simulating a penetration to see if there were identified weaknesses. We would look at their policies and procedures, similarly, to look for weaknesses.

So it's reactive work, something bad has already happened, we go in and assist them, or proactive work, providing services in advance to help them identify weaknesses and to make them better prepared to defend their environment.

MR. CASTRO: And what's the range of clients you have? For example, is it Fortune 500 companies? Is it universities, government agencies, individuals? What's the range of those?

MR. HENRY: I would say all of those. Not many individuals. There are some high-net-worth people that we've worked with or for. But primarily corporations across every sector: healthcare, financial services, manufacturing.

MR. CASTRO: Okay.

And, in general terms, what relationship does CrowdStrike maintain with law enforcement -- for example, the FBI -- or other government entities with cybersecurity resources, such as Department of Homeland Security?

MR. HENRY: We will engage with those agencies at the request of a client. Or if a law enforcement agency were to contact us, we would work with the client to facilitate what the law enforcement agency would need. It's not typical for us to engage with law enforcement in our engagements. It's not a typical relationship.

MR. CASTRO: How do you handle a situation where you do find out that somebody's been hacked? Do you reach out to the FBI or DHS? Do you allow the client to make that decision? What's your protocol there?

MR. HENRY: We would not unilaterally make that decision. If we did that, it would be at the client's request or in consultation with the client.

MR. CASTRO: You've made recommendations?

MR. HENRY: I have made recommendations.

MR. CASTRO: How about in this case?

MR. HENRY: In this case --

MR. CASTRO: Understanding that the FBI was already talking to the DNC.

MR. HENRY: So, in many cases, we're working under privilege with counsel, and we have to -- we respect that privilege, and we coordinate with counsel to do that.

MR. CASTRO: Prior to the 2016 campaign, had CrowdStrike done work for any political parties or election campaigns -- RNC, DNC, or any other political organizations?

MR. HENRY: Prior to?

MR. CASTRO: Prior to the 2016 work -- or prior to the DNC work in 2016.

MR. HENRY: I want to be clear on what the clarification of a political organization is.

MR. CASTRO: Whatever you consider it to be.

MR. HENRY: Well, that's the question.

MR. CASTRO: You know, the RNC, the DCCC, any State parties, for example, the Texas Democrats, the Texas Republicans, anything like that.

MR. HENRY: I'm not aware, prior to the DNC, of us being engaged with any political party. I'm not aware. But we have hundreds of engagements. But I'm not aware of any.

MR. CASTRO: Okay.

So, during your time at CrowdStrike, had you or your company identified any noteworthy trends or evolution in the offensive cyber operations of nation-state actors -- say, moving away from run-of-the-mill espionage towards more kinetic ops or outright active measures?

MR. HENRY: So I want to be clear again, because this is an important question. During my time at CrowdStrike --

MR. CASTRO: Yes.

MR. HENRY: -- were we aware of nation-states moving away from pure espionage to more kinetic-type attacks?

MR. CASTRO: Yeah. I mean, my question is meant to get at what trends you're seeing. For example, at least for many of us, this was the first time where we saw that emails or data were weaponized and used in the political arena. Had you seen that before? Or what kind of trends were you seeing such as that that you might be -- because one of the main charges of this committee is to make recommendations about how, going forward, as a Nation, we protect ourselves in the future from this kind of activity. But, first, we have to fully understand what was happening and going on.

MR. HENRY: No, I understand that. And I appreciate that question, because, as an American, I have the same concerns.

When you talk about weaponization, I think we have seen nation-states moving towards more destructive attacks. And the two that I would call out that

have been publicized are North Korea and Iran, both, where some of those actions have been publicized and acknowledged by the U.S. Government.

MR. CASTRO: Let me ask you, in terms of response by commercial clients -- or let me ask it this way so you don't have to divulge any of what your clients may have reacted or not reacted.

But just in terms of what you've seen as somebody who's got an expertise in this area, have commercial clients handled this differently than, say, a political client or government agency or so forth?

For example, we just found out in the news a few weeks ago that Uber -- I don't know whether they're a client or not -- but Uber paid some hackers $100,000 ransom, basically, and then didn't tell anybody for a year that it had happened. So it sounds like they certainly didn't go to the FBI or weren't talking to the FBI.

So what kind of responses have you seen from both commercial and noncommercial groups?

MR. HENRY: I think it ranges from groups that are completely unengaged, disengaged, to groups or organizations that are very aware and very engaged and applying the appropriate resources and a sense of urgency. It runs the gamut. I've seen it for many years that way.

I've talked to this committee about this before, in my prior position, and some of the things that we should all be doing differently and better. I'd be happy to come back and talk about that again.

MR. CASTRO: Let me ask you, because you are an expert, what recommendation do you have for what kind of responsibility a company or a government or the DNC or anybody else who's got large volumes of data, what responsibility, going forward, do you think that these organizations should have?

Should Congress pass a law that says that there's got to be some minimum level of cybersecurity? Because you just mentioned, of course, that there's some businesses, for example, that really don't take any precautions and are sitting ducks.

So, not with respect to your clients or anybody else but just as an expert, what do you recommend? Because this will be about recommendations.

MR. HENRY: I think, Mr. Castro, I really appreciate the question, and I do have an interest in this. I've been in this space for a long time, and I have a lot of concerns for our country. And I think, for the purposes of this, we're focused on this issue, and I would be happy to come talk about that issue, if I may, in a separate meeting, if that would be okay.

MR. CASTRO: Sure.

So, prior to 2016, was CrowdStrike tracking or observing the cyber threat posed by Russia?

MR. HENRY: Yes, sir.

MR. CASTRO: And how have you assessed Russian capabilities?

MR. HENRY: They are --

MR. CASTRO: How do they stack up against ours? In the world?

MR. HENRY: I'll say that they are among the best in the world. I won't compare them. I'll say they are among the best in the world.

MR. CASTRO: And what makes them among the best in the world?

MR. HENRY: Their tactics, their -- the techniques, the tools they've developed, their ability, their operational security, their rigor, I think their collection, their targeting -- a whole host of capabilities I'd look at from an intelligence perspective. And I think that they are tops in the world.

MR. CASTRO: What are their motives, as far as you can tell?

MR. HENRY: Well, I think, when we're looking at nation-states -- I mean, you're asking a geopolitical question, I think. And their motives are like other nation-states, to gain an advantage tactically in global policy, global politics, global economics. I think at a high level that's fair. We can go into it a lot deeper.

MR. CASTRO: Is it fair to say that Russia's ambition has grown over the last several years in that realm?

MR. HENRY: I mean, again, that's kind of a geopolitical issue, and it would be speculation, I guess.

MR. CASTRO: Okay.

Who is Fancy Bear?

MR. HENRY: Fancy Bear is an actor that we associated with Russian intelligence. It's likely a group of people that are operating on behalf of a Russian intelligence service, and aggregately we have named them Fancy Bear as a way for us to kind of identify different tactics and associate it with a particular group.

MR. CASTRO: They have a unique set or similar set of tactics they use that you can use to group them together or identify a group of individuals?

MR. HENRY: Yes.

MR. CASTRO: How about Cozy Bear?

MR. HENRY: A group, similarly, we have associated with Russian intelligence, and using different types of tactics, different tools, different target sets, but that we've also associated similarly with Russian intelligence.

MR. CASTRO: Is there an important distinction between those two groups?

MR. HENRY: I think that Fancy Bear has been associated with Russian

military based on a lot of the targeting, the types of intelligence that's been collected, and that Cozy Bear, not clear specifically which agency but more of a traditional intelligence collection organization.

So, in the case the DNC, for example, Cozy Bear was monitoring communication channels, looking at email, looking at voice-over-IP communications, sort of traditional intelligence collection.

MR. CASTRO: And I was going to ask you next about the role of Fancy Bear and Cozy Bear with respect to the DNC incident. Can you describe their role in all of this?

MR. HENRY: Yes. Cozy Bear I've just described. Fancy Bear was targeting the research, opposition research, candidate research. So some of the data that we saw staged but we didn't have indication that it was exfil'd, but it was staged -- appeared to be staged for exfil, that it was associated with research that had been conducted by the DNC on opposition candidates.

MR. CASTRO: And so you saw these two groups seem to divide up responsibility for activity?

MR. HENRY: Well, it's interesting. So we don't have any reason to believe that they actually were coordinating with each other. One of our analysts actually said that he didn't think that they were coordinating and that the Fancy Bear actor actually had been in the DCCC and had moved from the DCCC into the DNC environment, and that Cozy Bear had been there since July of 2015 and Fancy Bear didn't come into the environment until the end of April of 2016, so that Cozy Bear had been there for many months prior to Fancy Bear ever getting there.

MR. CASTRO: So your analysts who gave this report may have believed that these two Russian cells were operating independently of each other,

possibly?

MR. HENRY: Yes.

MR. CASTRO: And as a cybersecurity expert and a former FBI executive assistant director focused on cyber issues, heading into the start of the 2016 campaign, would you have had any particular concerns about the cybersecurity or digital integrity of U.S. political campaigns?

MR. HENRY: I have concern about the integrity of every network in this country.

MR. CASTRO: Any special concern about these political organizations?

MR. HENRY: I have concern about all critical infrastructure in this country. Yes.

MR. CASTRO: And do you recall any prominent foreign-sponsored cyber attacks or incidents of espionage against U.S. campaigns during the 2012 or 2014 election seasons?

MR. HENRY: Yes. I mentioned --

MR. CASTRO: Well, we talked about China back from '08.

MR. HENRY: -- the McCain and the Obama campaigns.

MR. CASTRO: But anything in 2012 or 2014, in that intervening period between 2008 and 2015?

MR. HENRY: Oh. I'm not aware. I'm not aware. I'd left the Bureau by the 2012 -- 2012? Yeah.

MR. CASTRO: Let me ask you, why do you think they did a document or data dump in 2016? Why not before that? Just as an expert.

MR. HENRY: So, to be clear, on the document dump, as you've referred to it, there was data that we know was taken off of the DCCC. And we've, I think,

chronicled, documented that in the report. There is evidence of exfiltration, not conclusive, but indicators of exfiltration off the DNC.

As the person who led the investigation into both of those remediations, I can state those facts. I don't know that I should speculate on why it may have been done.

So we did look at hash values, so algorithms of the documents that the FBI had provided, and compared that with documents that came off of the DNC, and they were consistent.

MR. CASTRO: Okay.

I'm going to pass it over to Mr. Swalwell. Thank you.

MR. HENRY: Thanks.

MR. SWALWELL: Thank you, Mr. Henry, for your participation. And we'll take a break, also, shortly, if you need one.

In your experience as an FBI agent, particularly in cyber notifications, if the Bureau learned that a corporation or entity had been penetrated, was there a standard protocol for how you'd contact that entity?

And we'll just stick with 2012, and then you can talk about what you observed in the private sector.

MR. HENRY: Yes, there was.

MR. SWALWELL: And what was it?

MR. HENRY: So it depends. I mean, notification would be made to a corporation that there was a breach into their environment. And we'll have to go back and pull what the document says specifically. But it depends on where the information came from.

We're in an unclassified environment. The FBI is a domestic intelligence

agency, and the FBI works domestically, and they coordinate with others in the community. And depending on where the intelligence came from, the FBI would be restricted on releasing certain pieces of data.

MR. SWALWELL: And looking at your experience from 2012 to present day, have you noticed a pattern or a manner of practice that the FBI has had in who they notify of your clients, like, which individuals at the companies are notified when a breach occurs? And I'll just give you an example. Is it the CTO? Is it, you know, someone at the IT help desk? I mean, what is typically the practice you've observed recently?

MR. HENRY: Again, it depends. If the FBI has an established relationship with somebody -- and that's encouraged. I mean, I'd recommend people in the private sector to have those contacts in advance of a breach. They would reach out to the person they've got an established contact with.

If they don't, it might be at the general counsel's office. It might be to the CISO, the chief information security officer. It depends on who you've got a relationship with. I don't know that the notification that you refer to is that explicit. I think it's case by case.

MR. SWALWELL: Sure.

In this case, the notification went to Yared Tamene, who you referenced earlier, an IT contractor for the DNC. Can you just, based on your experience, is that the -- had you been working at the Bureau, is that who you would've contacted first?

MR. HENRY: My understanding is that it was Yared that was contacted based on the document I referred to. I don't have any indication that anybody else was notified.

MR. SWALWELL: And I guess my question is, you know, he was an IT contractor for the Democratic National Committee that has a chairperson, a finance team, a political director. Are there other individuals who you believe may have been more appropriate to contact?

And, again, I'm asking you, you know, as an expert, not as somebody who performed work for the DNC, but just knowing what you know from working at the FBI and your work on this case.

MR. HENRY: I think that -- I mean, my role in this case was as leading the team that was responding. Pursuant to our contract with counsel, I don't know that I should speculate about --

MR. SWALWELL: Sure. I understand.

When Mr. Tamene was contacted in September 2015, it was by Special Agent [redacted] Is that right?

MR. HENRY: Yes.

MR. SWALWELL: Did you ever talk to Special Agent [redacted]

MR. HENRY: I have. I have spoken to him since the notification to the Bureau in June. And I may have spoken to him beforehand when I worked in the Bureau. I don't have a recollection of that.

MR. SWALWELL: Sure. And with respect to this case, what has Special Agent [redacted] conveyed to you, in an unclassified manner, about his contact with Mr. Tamene back in September 2015?

MR. HENRY: I don't know that I -- I don't recall talking to him specifically about his contact with Tamene. I may have talked to him about that. I don't recall specifically what the content of that would've been.

MR. SWALWELL: Sure. Great.

And I'll yield back.

MR. STEWART OF UTAH: Mr. Henry, thank you.

MR. CONAWAY: Do you need a break?

MR. HENRY: I'm okay. Thanks.

MR. STEWART OF UTAH: So we'll press ahead then.

MR. CONAWAY: Yeah, 15 minutes.

MR. STEWART OF UTAH: I yield to the chairman.

MR. CONAWAY: Oh, okay.

Again, Mr. Henry, thank you for being here. My professional background is as a CPA, so my questions are more slanted that direction. And I'm not a lawyer. This may be a bit disjointed because I'm kind of falling in on questions that were asked to you.

On your work on behalf of the DNC through Perkins Coie, did you do that on site? All remote? How did that mechanically work?

MR. HENRY: Both.

MR. CONAWAY: Both?

MR. HENRY: On site and remotely.

MR. CONAWAY: All right. And the team that made up your guys there, can you give us some general description of what their professional backgrounds are?

MR. HENRY: Yes. And I'll just caveat that. I can talk about the members of my specific team. Even though I was overseeing this incident, there are other members of our team that fall -- intelligence analysts and other members that come under different groups in my organization. So I don't know specifically --

MR. CONAWAY: The guys that are doing the cyber forensics, what do they look like?

MR. HENRY: Former U.S. Government, a couple of them.

MR. CONAWAY: FBI?

MR. HENRY: No. DOD, military.

MR. CONAWAY: NSA?

MR. HENRY: NSA. And former contractors or employees of defense contractors. Extensive experience in this area, in computer forensics and in working in this type of an environment.

MR. CONAWAY: All right. So you mentioned Tamene was the contractor who did -- was there another contractor, anybody else that you knew?

MR. HENRY: I only know Tamene that worked at MIS. I think there were other employees that worked with him. I don't recall ever meeting anybody there.

MR. CONAWAY: All right.

So, from an outsider looking in, he starts being contacted in September. When did he actually tell his client that something was going on? There doesn't seem to be a sense of urgency on his part. Any sense of why that's the case?

MR. HENRY: I don't know. And I don't know when he told anybody in the DNC. My only knowledge of the communications between him and the FBI were based on my looking at that document, April 30th or May 1st. And I don't remember if, in the document, it said that he told any of his superiors or anybody actually in the chain of command at the DNC.

MR. CONAWAY: All right.

So is it coincidental, then, that the data prepped for exfiltration on the 22nd

and then you being contacted by Perkins Coie? When did he tell the DNC that they had a problem? Or was it he contacted Perkins Coie on behalf of DNC? Any idea?

MR. HENRY: I don't know who in the DNC contacted Perkins Coie. I don't know who made that contact.

MR. CONAWAY: But it would have been them, not the contractor?

MR. HENRY: I would be speculating. I would assume so, but I'm speculating.

MR. CONAWAY: Had the contractor got a sense that something bad was about to happen on the 22nd, and that's why he escalated?

MR. HENRY: Again, to Mr. Stewart's question earlier, I don't know whether Michael Sussman said, you know, we have some indication or --

[Discussion off the record.]

MR. HENRY: As it relates to the notification to Perkins Coie, I don't know what that was.

MR. CONAWAY: Okay. I was worried that I wouldn't ask you a question that your attorney wouldn't pull you aside. Everybody else has, and so I was a little nervous that I would be so inane with my questions that you're over there laughing at me, but -- okay.

When you imaged and/or sent data to the FBI, did you filter anything out of that that the DNC would not have wanted the FBI to look at?

MR. HENRY: No, sir. I don't think so.

MR. CONAWAY: Okay.

MR. HENRY: No. And I say that because I know that part of our report is redacted, but I have no -- my understanding is everything we gave to the FBI was

as we collected it.

MR. CONAWAY: All right.

What is your obligation and your role as a contractor with a client like that, when you come across -- I mean, all of us have people who work for us that we don't supervise moment to moment that are potentially subject to looking at a website they shouldn't look at or having something on a company computer they shouldn't have.

Do you have any kind of responsibility -- when you go into that environment and you find something inadvertently that's not supposed to be there, what's your responsibility to that?

MR. HENRY: I don't understand the question.

MR. CONAWAY: I'll be a little more graphic. We've got somebody who's an employee -- you have an event that you've been called in to look at, and you find an employee who has downloaded child pornography onto a company computer. Are you under any obligation to tell the authorities or the client? What's your protocol in that regard? Or would you find that?

[Discussion off the record.]

MR. HENRY: If I found child pornography on a client's computer, yes, I would notify law enforcement.

MR. CONAWAY: Okay. Is that just a personal -- and it doesn't have to be something that heinous, but illegal. Is that just something you, as a, you know, code of conduct, would do? Or is there some sort of legal requirement for you do that?

MR. HENRY: There are legal requirements.

MR. CONAWAY: Okay. And with respect to your work at the DNC, you

observed all your legal requirements in that regard?

MR. HENRY: I didn't find child pornography.

MR. CONAWAY: Well, good. I wasn't going to ask you that bluntly, but nothing that would have caused them a problem?

MR. HENRY: Not that I'm aware of, sir.

MR. CONAWAY: Okay.

MR. STEWART OF UTAH: Can I refine that very quickly?

MR. CONAWAY: Sure.

MR. STEWART OF UTAH: He used the example of child pornography, but what about just any illegal activity? Are you required to report any illegal activity that you find on a client's computer?

MR. HENRY: I won't speculate on what my legal obligations are.

MR. STEWART OF UTAH: Okay.

MR. CONAWAY: In talking about the folks that you attribute these hacks to, you mentioned State Department and the Joint Chiefs of Staff hacks. How did you come by that information? Were they your clients as well, or is that just public reporting? Or how is it that you knew that the footprints, the fingerprints, the dust from those attacks were the same as at DNC?

MR. HENRY: Some of that, I believe, was public reporting, and I believe my team has had some access to some of the State Department reporting.

MR. CONAWAY: All right. In enough detail that you're confident that it's referring to both of those?

MR. HENRY: Yes, sir.

MR. CONAWAY: We use the phrase "the Russians did it" or "state actors." Can you be more precise? You said Cozy Bear was -- and I get them mixed up.

One of them was the military.

MR. HENRY: GRU.

MR. CONAWAY. Say that again?

MR. HENRY: GRU? Russian military intelligence? Fancy Bear.

MR. CONAWAY: All right. And Cozy Bear is?

MR. HENRY: Was a Russian intelligence service. Unclear --

MR. CONAWAY: As to which one?

MR. HENRY: Yes, potentially. I mean, there's other intelligence services that are Russia SVR and FSB. Not clear.

MR. CONAWAY: Okay.

Is anybody out there good enough, I guess, for lack of a better phrase, to run a false-flag operation using the exact same tactics, techniques, and procedures that Cozy Bear, Fancy Bear used that would have, in other words, caused us to look at the Russians and it was actually some other group doing it? Is anybody that good yet?

MR. HENRY: So, if you'll recall when I talked earlier about attribution, you look at data over the course of many intrusions over many years, and some of the infrastructure that we saw and some of the specific tactics and tools we've only seen associated with this particular actor, and it goes back many years.

MR. CONAWAY: Right.

MR. HENRY: So for somebody to do a false flag, as you've described it, it would've, I imagine, have been in play for many years. They would've had to have acquired Russian command-and-control servers. They would've had to somehow acquire tools and software, malicious code that had been used up until this point only by what we believe was the Russian Government.

MR. CONAWAY: Right.

MR. HENRY: So I don't think that that is plausible.

MR. CONAWAY: Right. But not totally impossible either, given the constant development of folks getting better and better.

MR. HENRY: I think that -- I don't think it's a viable option --

MR. CONAWAY: Okay.

MR. HENRY: -- under the circumstances here.

MR. CONAWAY: So you mentioned that Fancy Bear moved from DCCC to DNC?

MR. HENRY: Yes, sir.

MR. CONAWAY: What's your relationship to DCCC?

MR. HENRY: We also did an incident response at the DCCC.

MR. CONAWAY: All right.

MR. HENRY: After the DNC.

MR. CONAWAY: And so, talking about that movement sometime after June 10th?

MR. HENRY: It was prior to that, during the course of the response to the DNC incident.

MR. CONAWAY: Are they a similar relationship through Perkins Coie, or is that relationship through somebody else?

MR. HENRY: Yes, sir, same relationship.

MR. CONAWAY: Okay. And there you were able to tell the amount of data that was exfiltrated?

MR. HENRY: In that particular case, we were able to identify, based on some of the indicators that we saw, that there was data that was exfiltrated from

that network.

MR. CONAWAY: And you could attribute the total volume through some sort of metric?

MR. HENRY: So we can -- I mean, we saw an identified volume. I don't know that we can say that that's all that was taken, but we certainly can say what we saw, 70 gigabytes of data.

MR. CONAWAY: Okay.

And I apologize for not having the article with me. There is this conspiracy theorist group out there that will argue that you guys are just totally wrong and that it was an insider job, and they walk through this analysis using, quote/unquote, "experts," et cetera, et cetera. And the genesis of what they're arguing is that there's not a datalink out there fast enough to download what was believed to be downloaded without it being onto a thumb drive directly off the machine.

Have you seen that line of logic, or have you heard anybody talking about that?

MR. HENRY: I have seen it.

MR. CONAWAY: Okay. Do you find it plausible or implausible? What's going on with that conspiracy theory?

MR. HENRY: I've talked to the technical experts in my organization who say it's not plausible at all, what they're saying, that their argument is not plausible.

MR. CONAWAY: All right. And I'm skeptical of the article, as well, just because of all the other things that are going on that kind of back up what CrowdStrike did. The mechanics of download speeds, all the other things they talked about, which sounds very credible to the uninitiated, to someone who's looking at it without any kind of background, does it fall apart there? Where does

it fall apart when you talk to your guys?

MR. HENRY: I don't know that I can tell you the specifics about it, other than I've spoken to my team about it, who are true experts in this area, and they say that the argument is just not plausible.

MR. CONAWAY: Okay. He names some of the -- well, he doesn't either. Okay.

So what's your relationship with the Podesta emails?

MR. HENRY: I never -- I don't have a relationship with them, other than --

MR. CONAWAY: So that fishing expedition and the stealing of those was totally outside your realm or your work?

MR. HENRY: Yes.

MR. CONAWAY: Okay.

Did the DNC restrict anything that you shared with the FBI or that the FBI asked for? Did they tell you "no" at any point?

MR. HENRY: No, I have no recollection. Again, I know that there are redacted reports and there was some restriction on the reports. That's the only thing I can recall.

MR. CONAWAY: All right.

You mentioned that you left tools in --

[Discussion off the record.]

MR. HENRY: Everything that was requested by the FBI we provided.

MR. CONAWAY: Okay.

Quickly, you said you left tools in place to monitor for further intrusions. Is that a normal part of your service on remediation, that you leave those?

MR. HENRY: Yes, sir.

MR. CONAWAY: How long does that -- do they just stay in place permanently or as long as --

MR. HENRY: Prophylactically, yes.

MR. CONAWAY: Okay.

MR. HENRY: I mean, it's a service that we provide, so it's an ongoing service

MR. CONAWAY: Okay. And those are remote triggers, that if it happens, you get a notification?

MR. HENRY: Essentially. It's more complex, but that's essentially what we do.

MR. CONAWAY: I got you. You wouldn't necessarily wait on the contractor to call you and tell you something had triggered?

MR. HENRY: We would -- depending on the service, we would know that something happened.

MR. CONAWAY: Okay.

Does the FBI ever subcontract to you to do the investigations that they would've normally done? In a situation where they don't have enough manpower --

MR. HENRY: They have not subcontracted with us.

MR. CONAWAY: Have they contracted with you to do investigations? Maybe I used the wrong word.

MR. HENRY: They have not.

MR. CONAWAY: Okay.

And so the body of stuff that was prepped to be stolen, you can't unequivocally say it was or was not exfiltrated out of DNC, from what you know of?

MR. HENRY: I can't say based on that. But I think I said earlier that there was some -- and I want to make sure I'm correct here -- that there were some hash values, which are algorithms essentially, that were provided by the FBI that were consistent with files that were on the DNC. I think that that is accurate.

MR. CONAWAY: So how did the FBI get those if they didn't get them from you?

MR. HENRY: I don't know.

[Discussion off the record.]

MR. HENRY: They had gotten them from documents that had been dumped, and then they created the hash value, the algorithm.

MR. CONAWAY: Oh, it was dumped into the public arena?

MR. HENRY: Yes, sir.

MR. CONAWAY: Oh, I got you. Got you, got you.

All right. Your 15.

MR. SCHIFF: Thank you, Mr. Chairman. Just a couple of questions, and then I want to hand it back to Mr. Swalwell.

You mentioned that the hackers hacked the DCCC and then migrated from the DCCC to the DNC. Is that correct?

MR. HENRY: Cozy Bear was in the DNC. Our first identification of them in the DNC that indicated they were there was July of 2015. The second actor, Fancy Bear, migrated from the DCCC to the DNC.

MR. SCHIFF: And were you able to determine the original point at which Fancy Bear entered the DCCC?

MR. HENRY: We were not able to determine the original origin.

MR. SCHIFF: And at what point did they migrate from the DCCC to the

DNC?

MR. HENRY: In April of 2016. I had April 11th, I believe. Again, it's in the report. I'm not certain of the exact date, but I believe it's April 11th.

MR. SCHIFF: And you weren't retained to handle the intrusion into the Podesta emails?

MR. HENRY: No. No, I don't -- no.

MR. SCHIFF: Do you know who was?

MR. HENRY: I don't know. I don't think we did anything with that, no.

MR. SCHIFF: So you didn't have any interaction with them to determine the similarities or cyber signatures or digital dust that you saw in connection with DCCC and DNC and what they might have seen with respect to the Podesta hack?

MR. HENRY: No.

MR. SCHIFF: All right.

Mr. Swalwell?

MR. SWALWELL: Thank you.

You talked about the images you provided to the FBI with respect to the DNC hack. Is that common practice in your industry when the FBI is conducting an investigation and a third-party vendor, cybersecurity vendor like CrowdStrike is involved, that, rather than turning over a server, images would be sufficient?

MR. HENRY: I have done it before, or indicators at least, not necessarily a full image. But we have provided indicators in the past to the FBI in a case where an adversary was in a client's environment

MR. SWALWELL: And, in this case, is it fair to say that the DNC, being a rather large political entity, that at the time of its hack, or at the time that you were

working on the analysis and the remediation, that the DNC servers were still functioning for other purposes, that it was still an active operation that had email correspondence and web service hosting and other functions that were occurring? Is that right?

MR. HENRY: Yes.

MR. SWALWELL: Can you describe how disruptive it would be to turn over custody of your servers to the FBI for a client like that or any other client in a situation like this?

MR. HENRY: How disruptive it would be to turn over?

MR. SWALWELL: Well, I guess my question is, when you hear in the public realm, you know, why didn't the DNC just turn over their servers to the FBI, and you're telling us that images, according to the FBI, were sufficient, just for argument's sake, what does turning over the servers to the FBI mean practically to an organization that is still functioning and relying upon those servers?

MR. HENRY: When I hear somebody say "turning over the servers," based on my experience, it's not turning over the actual server; it's an image of the server.

MR. SWALWELL: Okay. And, in your experience, comparing this case to other clients that you've had or in your work at the FBI, you believe that the images were sufficient for the FBI to understand what had occurred?

MR. HENRY: I believe that the FBI got everything that they asked for that related to the DNC from us. Everything that we had access to related to images and servers, when they asked for it, they got it.

MR. SWALWELL: How did you present your findings to the DNC? Was it by a report, or was it a --

MR. HENRY: It was by a report that I believe the committee has.

MR. SWALWELL: Who did you present your findings to?

MR. HENRY: I believe it was to Perkins Coie, to the law firm, because they were the client, essentially, right? We were contracted through the law firm.

MR. SWALWELL: One second, please.

I'll yield to Ms. Speier.

[4:00 p.m.]

MS. SPEIER: Thank you for being here.

Did you do any work on behalf of the RNC? And I apologize if this question was asked earlier.

MR. HENRY: So there are a number of political organizations that we have done work for. To the extent that they're protected under privilege, I want to be careful not to say anything that's protected. And so I don't know -- I don't know, honestly.

MS. SPEIER: Okay. But you've -- can we surmise from that that you have worked for both political parties?

MR. HENRY: You can surmise that we have worked for multiple political organizations on both sides of the aisle.

MS. SPEIER: Okay.

One of the findings of the Intelligence Community assessment that came out in January was that, while voter records were hacked in a number of States -- I think the number grew to over 20 States, maybe even higher -- with a fair degree of confidence, the IC believed that the actual voting machines had not been hacked.

Now, subsequently, there have been a number of conventions. One took place in Las Vegas called DEFCOM, where they purchased 10 different voting machines from around the country and proceeded to hack them, each and every one of them, over the weekend, one within the first hour and a half of the conference getting taken up.

I spoke to one of the hackers, and his comment to me was, there's no way you could know whether or not the actual election machine had been hacked or

not because of the way they're constructed.

Are you at all familiar with the ability to hack into election equipment?

MR. HENRY: No.

MS. SPEIER: And you weren't brought in to look at the hacking of voting records by the FBI or the IC community?

MR. HENRY: No.

MS. SPEIER: And you don't know who was brought in?

MR. HENRY: No.

MS. SPEIER: So you have no opinion on whether those two statements are accurate or not?

MR. HENRY: No.

MS. SPEIER: Okay. I'll yield.

MR. CONAWAY: Mr. Quigley?

MR. QUIGLEY: So a part of our concern here is making sure these things don't happen again. Just your general sense of the following thoughts.

Most entities don't know they've been hacked. Is that correct? Like, a corporation, Target, what have you.

MR. HENRY: That's a very general, when you say "most organizations don't know they've been hacked" --

MR. QUIGLEY: Most entities that are hacked don't know that they've been hacked. Someone else has to tell them.

MR. HENRY: I've notified many companies that they've been hacked that did not know they'd been hacked. I don't know that I would say most, because I don't know the universe of companies. But oftentimes companies don't know that they've been hacked.

MR. QUIGLEY: Okay. And oftentimes someone else who is more expert in such things has to be the one that tells them.

MR. HENRY: That happens regularly.

MR. QUIGLEY: And, in your experience, how long is the range of time before -- you know, from the time they've been hacked to the time that they've been told they've been hacked, how long have you witnessed that timeframe?

MR. HENRY: There are multiple analyses that have been done. The term is "dwell time," how long is an adversary in an environment before they're identified. I think, actually, our public reporting that is coming out in the next couple of weeks will say it's about 3 months. There have been other consultancies that have opined that it's in excess of that.

MR. QUIGLEY: So help me make this question more specific. The entities that we have now hacking, the adversaries who are hacking into government, into corporate U.S. interests, can we tell that they are there? Are the adversaries so good that we just don't know that they're there at this point?

MR. HENRY: It depends, sir, on which organization is looking at it. There are certain organizations that will never know because they don't have the sophistication or the tools, and there are other organizations who are much better prepared to know. So it really depends. There's too many variables to answer that.

MR. QUIGLEY: But are there adversaries who use sophisticated attacks so good that they just cannot be detected?

MR. HENRY: Well, you're asking me to prove a negative. And I'm not being a wise guy. If they can't be detected, I don't know if there's anybody ever been there or not.

I can say this -- and we had spoken prior -- about the sophistication of adversaries that we see now and their ability to remain obfuscated and to be surreptitious for long periods of time, and there are nation-states that we've witnessed that have that type of capability.

MR. QUIGLEY: So I know you're being very careful and cautious, and I appreciate and respect that. But you have a general understanding of the sophistication of local governments, I would assume. And are most State boards of election capable of having the sophistication you spoke of earlier to know when they've been hacked?

MR. HENRY: I don't know because I haven't done an evaluation of those organizations.

MR. QUIGLEY: Okay.

Thank you. I yield back.

MR. SWALWELL: Thank you.

And just to clarify as to Ms. Speier's questions and Mr. Quigley, you had stated earlier that you worry about all infrastructure, as far as vulnerability to a hack. Is that correct?

MR. HENRY: Correct.

MR. SWALWELL: And that would include election infrastructure?

MR. HENRY: Yes.

MR. SWALWELL: And just a few questions about APT-28 and APT-29. It's correct -- and I know you've turned over the report, but just for our record -- that it was April 18th, 2016, when APT-28 first appeared on the DNC servers. Is that correct?

MR. HENRY: What we call Fancy Bear, yes, APT-28.

MR. SWALWELL: Okay. And the system --

MR. HENRY: Wait. I'm sorry. To clarify, you said when they first showed up there?

MR. SWALWELL: Yes.

MR. HENRY: I thought that the date was April 11th. Again, it's in the report. I want to make sure that we're accurate.

MR. SWALWELL: And the systems compromised in your report included domain controllers, IT workstations, backup servers, donor information, voter file data, email, Voice Over Internet Protocol, shared drives, party affairs, accounting, marketing, and research. Is that right?

MR. HENRY: Yes, sir.

MR. SWALWELL: And Mr. Brown -- do you know Andrew Brown?

MR. HENRY: I know who he is, yes.

MR. SWALWELL: Okay. He has stated that "we didn't see any evidence that the attackers had gone after the data warehouse environment. They seemed to be completely focused on the DNC corporate network."

Do you agree or disagree with that statement?

MR. HENRY: I don't know what he was referring to.

MR. SWALWELL: And as far as activity that you would attribute to APT -- let me withdraw that.

And, Mr. Chair, I believe that we're assuming a lot of facts about this report, but can we enter the report as exhibit 1 for the record, the CrowdStrike report that's been referred to?

MR. CONAWAY: Without objection, it's admitted.

[Henry Exhibit No. 1

was marked for identification.]

MR. SWALWELL: Okay. Thank you.

One of the questions we're supposed to answer for the public is the sufficiency of the government response to the attack, meaning once the FBI learned about the attack, once the Obama administration learned about the attack, and then actions that were taken.

And just in your expertise as a former FBI agent with cyber expertise and working on the private sector, are there any recommendations you would make to the committee, based on your public knowledge and intimate knowledge, having worked partially in this investigation, as to what the government response could have been to have been more effective to stop this intrusion?

MR. HENRY: I'd be happy to have that conversation. I don't know -- I want to focus on the DNC here, if that's all right.

MR. SWALWELL: Sure.

MR. HENRY: And I would be happy to have that conversation.

MR. SWALWELL: And is that, in part, because it would involve conveying to us classified information?

MR. HENRY: Yes.

MR. SWALWELL: Okay. Thank you.

Anything else, Ms. Speier?

I yield back.

MR. STEWART OF UTAH: Thank you, Mr. Henry. And I have to say you've been an outstanding witness. You've been patient with us. Thank you for that. And you've been, I think, as forthright as you could be.

And it's been a couple hours now, so I think we'll be -- at least I think we'll

be concluding fairly shortly. I'd like to go through four questions, and they might be as simple as yes/no. It may not take much time, but elaborate, if you would.

Among your many clients, are you also under contract with the FBI to perform technical services for them?

MR. HENRY: No.

MR. STEWART OF UTAH: And never have been?

MR. HENRY: No.

MR. STEWART OF UTAH: Okay.

MR. HENRY: We have not provided them technical services. We have provided them intelligence in the past.

MR. STEWART OF UTAH: Okay. As part of a contract or just part of a professional courtesy that you share that type of information?

MR. HENRY: We did it as part of a contract.

MR. STEWART OF UTAH: Okay. Are you currently under contract to provide that information to them?

MR. HENRY: I do not think so.

MR. STEWART OF UTAH: Okay.

You said something, and I want to restate it -- and tell me if I'm wrong -- if I could. You said, I believe, talking about the DNC computer, you had indications that data was prepared to be exfiltrated, but no evidence it actually left.

Did I write that down correctly?

MR. HENRY: Yes.

MR. STEWART OF UTAH: And, in this case, the data I am assuming you're talking about is the email as well as everything else they may have been trying to take.

MR. HENRY: There were files related to opposition research that had been conducted.

MR. STEWART OF UTAH: Okay. What about the emails that everyone is so, you know, knowledgeable of? Were there also indicators that they were prepared but not evidence that they actually were exfiltrated?

MR. HENRY: There's not evidence that they were actually exfiltrated. There's circumstantial evidence --

MR. STEWART OF UTAH: Okay.

MR. HENRY: -- but no evidence that they were actually exfiltrated. But let me also state that if somebody was monitoring an email server, they could read all the email.

MR. STEWART OF UTAH: Right.

MR. HENRY: And there might not be evidence of it being exfiltrated, but they would have knowledge of what was in the email.

MR. STEWART OF UTAH: But they wouldn't be able to copy that email; they could only watch it in real-time.

MR. HENRY: There would be ways to copy it. You could take screenshots. You could copy it.

MR. STEWART OF UTAH: All right. So I think that's one of the more interesting things that we've learned from you today, again, that there is no evidence it was actually exfiltrated.

Is it -- it seems unlikely to me that in the real-time that they're watching these emails that they'd be able to collect the hundreds or thousands that they had but with screenshots or whatever.

MR. HENRY: So there is circumstantial evidence that it was taken.

MR. STEWART OF UTAH: I understand, but not conclusive.

MR. HENRY: We didn't watch it happen. There's not a network sensor that actually saw traffic actually leaving, but there's circumstantial evidence that it happened.

And, also, the Cozy Bear actor that I mentioned earlier that was in the environment going back to July of 2015, there were many months before we ever got there where data may have --

MR. STEWART OF UTAH: Okay. All right.

MR. HENRY: Again, speculating, but --

MR. STEWART OF UTAH: But you have a much lower degree of confidence that this data actually left than you do, for example, that the Russians were the ones who had breached the security?

MR. HENRY: There is circumstantial evidence that that data was exfiltrated off the network.

MR. STEWART OF UTAH: And circumstantial is less sure than the other evidence you've indicated. Circumstantial evidence is less sure than definitive.

MR. HENRY: So, to go back, because I think it's important to characterize this. We didn't have a network sensor in place that saw data leave. We said that the data left based on the circumstantial evidence. That was a conclusion that we made.

When I answered that question, I was trying to be as factually accurate. I want to provide the facts. So I said that we didn't have direct evidence. But we made a conclusion that the data left the network.

MR. STEWART OF UTAH: Okay. That's fair. But it gives us, kind of, context. Some things are more sure than others. And we appreciate that.

Any evidence that any entity other than Russia had access to the DNC servers?

MR. HENRY: We have no evidence of that.

MR. STEWART OF UTAH: Okay.

And then I think this is my last question. CrowdStrike cofounder -- I'm sure he's a friend of yours -- Dmitri Alperovitch, if I'm saying his name correctly, I understand he has a Russian background.

MR. HENRY: Yes.

MR. STEWART OF UTAH: Does that give him insights or background that helps in these types of investigations, or is he far enough removed from that that it doesn't really benefit you?

MR. HENRY: He left there when he was a boy.

MR. STEWART OF UTAH: Oh, okay. So he maybe speaks the language or something else, but no other --

MR. HENRY: Yes, sir.

MR. STEWART OF UTAH: -- no other real benefit. Okay. All right.

Mr. Chairman?

MR. CONAWAY: Okay.

MR. STEWART OF UTAH: Thank you. I'm going to have to leave, but, again, thank you for being here.

MR. HENRY: Thank you.

MR. CONAWAY: So the mechanics of Cozy Bear being set up there, they could be watching traffic go across in real-time? Is that the way that works?

MR. HENRY: Yes, sir.

MR. CONAWAY: And the Voice Over Internet Protocol, they could be

listening to the conversations like that?

MR. HENRY: Yes, sir.

MR. CONAWAY: Okay.

You know there was a body of data ready to go April 22nd, I think you said. Could that have happened previously during that timeframe and they erased the footprint of that having happened so you just -- or is it --

MR. HENRY: Yes.

MR. CONAWAY: Okay. So you're just aware of that one block that was ready to go, but you can't tell whether it went or not. But as long as they'd been on there, they could have periodically come in and gotten data?

MR. HENRY: Yes.

MR. CONAWAY: Because we didn't have any monitors on it, there wasn't any evidence?

MR. HENRY: Yes.

MR. CONAWAY: Okay.

Eric, anything else?

MR. SWALWELL: Mr. Henry, I know it's been about 5 years since you left the Bureau, but throughout the 20-some-odd years that you were an agent, did you ever testify in court?

MR. HENRY: Grand jury.

MR. SWALWELL: Okay. And do you remember ever presenting to the grand jury or being a part of jury instructions that told them that, in the court of law, circumstantial evidence can be treated the same as direct evidence if you believe that circumstantial evidence?

MR. HENRY: Have I heard that been said?

MR. SWALWELL: Yes.

MR. HENRY: Yes.

MR. SWALWELL: And DNA evidence is circumstantial evidence, isn't it?

MR. HENRY: In this case, we reached a conclusion that the evidence -- that the data left the network. That's the conclusion we came to.

MR. SWALWELL: And I just want to be clear, based on the last line of questioning, that you're not saying that circumstantial evidence in this case was weaker than direct evidence. It's just it was only circumstantial evidence that you could rely upon. Is that right?

MR. HENRY: Sir, I was just trying to be factually accurate, that we didn't see the data leave, but we believe it left, based on what we saw.

MR. SWALWELL: And the report that you provided to the DNC on August 24th, 2016, is there any information that you've learned since that report, based on dumps that have occurred, that inform you any further as to your findings in this case?

So, you know, time has passed since August 24th, 2016. Have you learned anything else, based on anything in the public realm, about what occurred?

MR. HENRY: I've heard the U.S. Intelligence Community say that this was Russia --

MR. SWALWELL: Okay.

MR. HENRY: -- after our report was completed.

MR. SWALWELL: But just so we're clear, there's nothing that you or your team have analyzed or looked at from, like, public dumpings by the Russians or Guccifer or WikiLeaks that changes your opinion or has supplemented your

opinion?

MR. HENRY: There's nothing that changes our opinion. We stand on our analysis, and we stand on our assessment --

MR. SWALWELL: Great.

MR. HENRY: -- that the Russian Government hacked the DNC.

MR. SWALWELL: I'll leave it at that, Mr. Chair.

MR. CONAWAY: Mr. Henry, thank you so very much. Appreciate that. It doesn't look like we have any other questions, but if we do, we might have to call you back.

But thank you. We're adjourned.

[Whereupon, at 4:18 p.m., the interview was concluded.]